

REMARKS

The Applicants appreciate the thorough examination of the present application that is reflected in the Office Action of October 5, 2004. In response, the Applicants have amended independent Claims 1, 13, 25, 37, and 38 to clarify that "each hash value for each of the plurality of data streams" is combined with a unique identifier of the application processing component which created the data stream. These amendments do not change the scope of the independent claims because the additional language merely restates an established relationship that a hash value is computed over each of a plurality of data streams, wherein each data stream is created by a different application processing component.

In addition, Claims 1-4, 6-8, and 10 have been amended to remove "means for" terminology; and Claims 25-28, 30-32, 34, 37, and 38 have been amended to remove "step" and/or "steps" terminology. The Applicants have also amended the specification to insert U.S. patent numbers and patent application numbers that are now available.

The Applicant will also show in the following remarks that all claims are patentable over the cited art. A Notice of Allowance is thus respectfully requested in due course.

Claim 1 Is Patentable Over The Cited Art

Claim 1 has been rejected under 35 U.S.C. Sec. 103(a) as being unpatentable over U.S. Patent No. 6,009,176 to Gennary *et al.* (Gennary) in view of U.S. Patent No. 5,666,415 to Kaufman (Kaufman) and in further view of U.S. Patent No. 5,923,763 to Walker *et al.* (Walker). In response, the Applicants will show that Claim 1 is patentable for at least the reasons discussed below.

In particular, Claim 1 recites a computer program product for digitally notarizing a collection including a plurality of data streams. More particularly, the computer program product is embodied on one or more computer-usable media and includes:

computer-readable program code configured to compute a hash value over each of the plurality of data streams, wherein each data stream is created by a different application processing component;

computer-readable program code configured to combine each hash value for each of the plurality of data streams with a unique identifier of the application processing component which created the data stream for which the hash value was computed, thereby creating a combination data block;

computer-readable program code configured to hash the combination data block;

computer-readable program code configured to digitally sign the hashed combination data block with a private cryptographic key, wherein the private cryptographic key and a public cryptographic key which is cryptographically associated therewith represent a digital notary; and

computer-readable program code configured to provide the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the collection plurality of data streams, wherein the digital notarization cryptographically seals contents of the collection of data streams. (Underline added.)

The Applicants respectfully submit that the cited references, taken alone or in combination fail to teach or suggest computing a hash value over each of a plurality of data streams created by different application processing components. The Office Action states that:

Gennaro discloses splits the streams into blocks and creates a table listing cryptographic hashes of each of the blocks (Gennaro:column 1, lines 23-27). This meets the limitation of "computer-readable code means for computing a hash value over each of the plurality of data streams, wherein each data stream is created by a different application processing component."

The Applicants respectfully disagree. In particular, the cited portion of Gennaro states that:

Another type of solution works only for finite streams. In this case, once again the stream is split into blocks. Instead of signing each block, the sender creates a table listing cryptographic hashes of each of the blocks. Then the sender signs this table. When the receiver asks for the authenticated stream, the sender first sends the signed table followed by the stream. (Underline added.)

Gennaro, col. 1, lines 23-27. Gennaro thus discusses a single data stream that is sent from a single sender. Accordingly, Gennaro fails to teach or suggest a plurality of data streams created by different application processing components, much less, computing a hash value over each of the plurality of data streams created by the different application processing components. While the Walker and Kaufman patents are cited with respect to Claim 1, the Office Action does not allege that any portions of these patents teaches a plurality of data streams created by different application processing components or computing a hash value over each of the plurality of data streams. Accordingly, the combination of Gennaro, Walker, and Kaufman fails to teach or suggest these recitations.

The Applicants further submit that the cited patents fail to teach or suggest combining each hash value for each of the plurality of data streams with a unique identifier of the application

processing component which created the data stream for which the hash value was computed. In particular, the Office Action concedes that:

Gennaro ... does not disclose "computer-readable program code means for combining each hash value with a unique identifier of the application processing component which created the data stream for which the hash value was computed...."

Instead, the Office Action cites Walker as disclosing these recitations. With respect to Figure 1 of Walker, Walker discusses a device for secure timestamping wherein:

a unique device identification number, stored in RAM 30 or memory 40, can be added to the hash to provide assurance of message authenticity.

Walker, col. 5, lines 54-55. Walker, however, does not discuss a plurality of data streams or unique identifiers for different application processing components creating the different data streams. Timestamping as discussed in Walker thus fails to teach or suggest combining each hash value for each of the plurality of data streams with a unique identifier of the application processing component which created the data stream wherein each data stream is created by a different application processing component. While the Kaufman patent is also cited with respect to Claim 1, the Office Action does not allege that any portion of this patent teaches combining hash values with unique identifiers. Accordingly, the combination of Gennaro, Walker, and Kaufman fails to teach or suggest these recitations.

Moreover, the Applicants submit that the cited patents fail to teach or suggest hashing a combination data block. In particular, the Office Action concedes that:

neither Genaro nor Walker disclose "computer-readable program code means for hashing the combination data-block."

Kaufman fails to provide the missing teachings. In particular, the cited portions of Kaufman discuss a Lamport Hash scheme wherein "the server holds data derived from the password by iteratively one way transforming it a large number of times...." (*See* Kaufman, col. 3, lines 21-23.) Kaufman thus discusses iterative transformations as opposed to hashing a combination data block. Accordingly, the combination of Gennaro, Walker, and Kaufman fail to teach or suggest these recitations.

As discussed in the Manual Of Patent Examining Procedure (MPEP), three basic criteria must be met to establish a *prima facie* case of obviousness. First, there must be some suggestion or

motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *See*, MPEP Sec. 2143.

As discussed above, the cited Gennaro, Walker, and Kaufman patents fail to teach or suggest:

- (1) computing a hash value over each of a plurality of data streams created by different application processing components;
- (2) combining each hash value for each of the plurality of data streams with a unique identifier of the application processing component which created the data stream for which the hash value was computed; and/or
- (3) hashing a combination data block

Moreover, there is no motivation to selectively combine aspects of signing digital data streams of Gennaro with aspects of timestamping of Walker with aspects of the Lamport Hash scheme of Kaufman.

Accordingly the Applicants respectfully submit that Claim 1 is patentable over the cited art. In addition, the Applicants submit that Claims 13, 25, 37, and 38 are patentable for reasons similar to those discussed above with respect to Claim 1. Moreover, Dependent Claims 2-12, 14-24, and 26-36 are patentable at least as per the patentability of Claims 1, 13, and 25 from which they depend.

Various Dependent Claims Are Independently Patentable

As discussed above, Dependent Claims 2-12, 14-24, and 26-36 are patentable at least as per the patentability of Claims 1, 13, and 25 from which they depend. Various of these dependent claims are also independently patentable.

For example, art has not been applied by the Office Action with respect to recitations of any of Dependent Claims 2, 3, 6-12, 14, 15, 18-24, 26, 27, or 30-36. More particularly, all claim recitations discussed in sections 3-7 of the Office Action are recitations from independent claims. Accordingly, the Applicants respectfully submit that each of these claims is independently patentable over the cited art. If any rejections should be maintained with respect to any of these dependent claims, the Applicants respectfully request application of art with respect to the

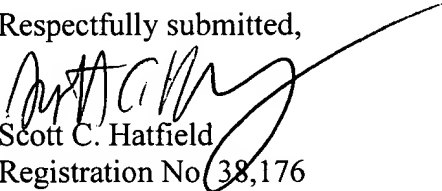
In re John R. Hind *et al.*
App.Ser.No. 09/764,541
Filed: January 17, 2001
Page 18

recitations of these claims in a non-final office action so that Applicants will have an opportunity to address any such rejections.

CONCLUSION

Accordingly, the Applicants submit that all pending claims in the present application are in condition for allowance, and allowance of all claims is respectfully requested in due course.

Respectfully submitted,



Scott C. Hatfield
Registration No. 38,176

USPTO Customer No. 46589
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401